



Electronic Banking Liability Application

For the purposes of this application, the term applicant means the parent company and all subsidiaries being proposed for coverage.

Parent Company: _____
 Web site address: _____ (city & state)
 IT Security Officer: _____

Requested Limit: \$ _____ Retention: \$ _____

	Yes	No
1. Does the applicant out source parts of its IT operations or systems (other than its connection to the internet), such as hosting its web site or internet banking functions? If yes, please attach a list of the service providers along with a description of the functions each provides. The definition of covered electronic systems is <u>not</u> extended to any service provider, unless the definition is so extended via endorsement.	<input type="checkbox"/>	<input type="checkbox"/>
2. Is there a current, centralized and documented IT security policy which includes defining the acceptable use of all company IT resources, including email and access to the internet?	<input type="checkbox"/>	<input type="checkbox"/>
3. Are all employees and contractors required to sign acknowledgement of the IT security policy and of your company's privacy policy?	<input type="checkbox"/>	<input type="checkbox"/>
4. Are all subsidiaries required to operate under the same IT security policies and procedures?	<input type="checkbox"/>	<input type="checkbox"/>
5. Does the IT infrastructure support proper compliance with the applicant's privacy policy?	<input type="checkbox"/>	<input type="checkbox"/>
6. Are employees, consultant and contract personnel informed about the proper process for reporting suspected security incidents?	<input type="checkbox"/>	<input type="checkbox"/>
7. Are IT employees and contractors subjected to criminal background checks as part of the hiring process?	<input type="checkbox"/>	<input type="checkbox"/>
8. Are firewalls used to prevent unauthorized access on all connections from internal networks and systems to external networks?	<input type="checkbox"/>	<input type="checkbox"/>
9. Are remote users authenticated before being allowed to connect to internal networks and systems?	<input type="checkbox"/>	<input type="checkbox"/>
10. Is all sensitive information encrypted when it is transmitted over external networks?	<input type="checkbox"/>	<input type="checkbox"/>
11. Are anti-virus software and procedures used on all personal computers including lap tops and desk tops and on all mission critical servers?	<input type="checkbox"/>	<input type="checkbox"/>
12. Are backup and recovery procedures in place for all mission critical systems?	<input type="checkbox"/>	<input type="checkbox"/>
13. Are backups taken at least once per week and stored off site?	<input type="checkbox"/>	<input type="checkbox"/>
14. Are recovery procedures tested at least annually?	<input type="checkbox"/>	<input type="checkbox"/>
15. Are there policies requiring that removable media containing sensitive information be properly labeled and protected against unauthorized access in effect?	<input type="checkbox"/>	<input type="checkbox"/>
16. Are Computer Emergency Response Team (C.E.R.T.) and vendor advisories related to security problems monitored and are corrections, such as software vulnerability patches or antivirus updates, applied as soon as possible to all affected systems?	<input type="checkbox"/>	<input type="checkbox"/>
17. Is there a network intrusion monitoring system in place?	<input type="checkbox"/>	<input type="checkbox"/>
18. Are there documented incident management processes to respond to suspected intrusions?	<input type="checkbox"/>	<input type="checkbox"/>
19. Are the employees, designated to respond to suspected intrusions, trained in the handling of forensic evidence, law enforcement involvement and press relations?	<input type="checkbox"/>	<input type="checkbox"/>
20. Are customers and other external users authenticated through the use of PINS, passwords or digital certificates?	<input type="checkbox"/>	<input type="checkbox"/>
21. Are employees and all internal users required to change their passwords at least every 90 days?	<input type="checkbox"/>	<input type="checkbox"/>
22. Are special privileges restricted to primary and backup systems administration personnel?	<input type="checkbox"/>	<input type="checkbox"/>
23. Are procedures in place to ensure that the passwords and privileges of terminated employees and contractors are immediately revoked?	<input type="checkbox"/>	<input type="checkbox"/>

	Yes	No
24. Are all IT equipment and terminals in areas protected from unauthorized access?	<input type="checkbox"/>	<input type="checkbox"/>
25. Are continuity plans in place for all mission critical business processes including those provided by outside vendors?	<input type="checkbox"/>	<input type="checkbox"/>
26. Are business continuity plans tested at least once every 2 years?	<input type="checkbox"/>	<input type="checkbox"/>
27. Are there annual security reviews of IT systems, policies and procedures by internal audit or an independent IT security specialist? If yes, please attach a copy of the most recent audit report.	<input type="checkbox"/>	<input type="checkbox"/>
28. Are network vulnerability scans conducted at least semiannually to test the security of perimeter network controls such as firewalls, external routers, and remote access servers?	<input type="checkbox"/>	<input type="checkbox"/>
29. Does the applicant use wireless networks?	<input type="checkbox"/>	<input type="checkbox"/>
30. Are wireless transmissions encrypted?	<input type="checkbox"/>	<input type="checkbox"/>
31. Are any wireless LANS installed outside the applicant's firewall?	<input type="checkbox"/>	<input type="checkbox"/>
32. Have the default security features of your wireless network been activated?	<input type="checkbox"/>	<input type="checkbox"/>
33. Are wireless LAN keys changed immediately upon the knowledge of a lost or stolen laptop?	<input type="checkbox"/>	<input type="checkbox"/>
34. Are there regular wireless LAN audits to detect rogue wireless LAN connections?	<input type="checkbox"/>	<input type="checkbox"/>
35. Are wireless LAN security policies documented and distributed to those employees given wireless capabilities?	<input type="checkbox"/>	<input type="checkbox"/>
36. Does the applicant conduct on-line trading?	<input type="checkbox"/>	<input type="checkbox"/>
37. If the applicant conducts on-line trading, is there an alternative means for its customers to request/effect trades in the event that its web site and/or on-line trading system are not functioning properly?	<input type="checkbox"/>	<input type="checkbox"/>
38. Does the applicant require its trading customers to sign a liability waiver?	<input type="checkbox"/>	<input type="checkbox"/>
39. Has the applicant failed to properly complete any trades in the past 3 years? If yes, please attach details including the amount of such trades, the reason(s) the trades were not properly completed and the corrective actions taken.	<input type="checkbox"/>	<input type="checkbox"/>
40. Has the applicant been criticized by any regulator regarding its computer operations in the past 3 years? If yes, please attach details including the corrective actions taken.	<input type="checkbox"/>	<input type="checkbox"/>
41. Has the applicant experienced a loss of IT service (except for planned maintenance or a natural disaster, such as flood, windstorm, earthquake, etc.) that exceeded 4 hours in the past 3 years? If yes, please attach details including the length of downtime, the cause of the disruption, the cost to restore service and the corrective actions taken.	<input type="checkbox"/>	<input type="checkbox"/>
42. Has the applicant experienced a security breach that resulted in unauthorized access to confidential data in the past 3 years? If yes, please attach details including the type and amount of confidential data exposed and the corrective actions taken.	<input type="checkbox"/>	<input type="checkbox"/>
43. Does the applicant have any knowledge of any situation which may develop into an electronic banking liability claim or loss? If yes, please attach details.	<input type="checkbox"/>	<input type="checkbox"/>

THE UNDERSIGNED DECLARES THAT THE STATEMENTS SET FORTH HEREIN ARE TRUE. THE UNDERSIGNED AGREES THAT IF THE INFORMATION SUPPLIED ON THIS QUESTIONNAIRE CHANGES BETWEEN THE DATE OF THIS QUESTIONNAIRE AND THE EFFECTIVE DATE OF THE INSURANCE, HE/SHE (UNDERSIGNED) WILL IMMEDIATELY NOTIFY THE INSURANCE COMPANY OF SUCH CHANGES, AND THE COMPANY MAY WITHDRAW OR MODIFY ANY OUTSTANDING QUOTATIONS AND/OR AUTHORIZATION OR AGREEMENT TO BIND INSURANCE.

NOTICE: IN SOME STATES, ANY PERSON WHO KNOWINGLY AND WITH INTENT TO DEFRAUD ANY INSURANCE COMPANY OR OTHER PERSON FILES AN APPLICATION FOR INSURANCE CONTAINING ANY MATERIALLY FALSE INFORMATION, OR CONCEALS, FOR THE PURPOSE OF MISLEADING, INFORMATION CONCERNING ANY FACT MATERIAL THERETO, COMMITS A FRAUDULENT INSURANCE ACT, WHICH IS A CRIME. REFER TO APPLICATION COMPLETED WITH THE ORIGINAL BOND OR POLICY FOR STATE SPECIFIC FRAUD STATEMENTS TO APPLICANTS.

Applicant: _____

By: _____
Signature and Title

_____ Date